(12) UK Patent Application (19) GB (11) 2 067 871 A

(21) Application No 8039388
(22) Date of filing 9 Dec 1980
(30) Priority data
(31) 80/01832
(32) 19 Jan 1980
(33) United Kingdom (GB)
(43) Application published
30 Jul 1981
(51) INT CL³
H04N 7/16 5/76
(52) Domestic classification
H4F D12M D12X D13A
D30K DE
(56) Documents cited
GB 1503051
GB 1474597
GB 1159610
GB 1001442
GB 1001441
GB 929251
GB 917591
GB 580167
(58) Field of search
H4F
H4R

(71) Applicant
The Marconi Company Limited,
Marconi House, New Street, Chelmsford, Essex
(72) Inventor
Robert James Evelyn Pollard
(74) Agent
J. P. L. Hooper,
The Patent Department, The Marconi Company Limited, Marconi House, New Street, Chelmsford, Essex

(54) Information Encoding Systems

(57) In an information encoding system for coded communication, successive blocks of the information e.g. video information, are pseudo-randomly scanned, the actual pseudo-random scanning sequence being changed from block to block according to a predetermined but "secret" key, the output from the scanning process constituting the information in coded form; and the thus-coded information is then distributed in a form which does not include any details which fully define the key, the required key-defining details being themselves distributed separately and independently. The decoding of the coded information is then only possible with a knowledge of the key identifying the particular pseudo-random scanning sequences used in the coding operation. The system is particularly applicable to the encoding of video tapes to prevent copyright infringement.

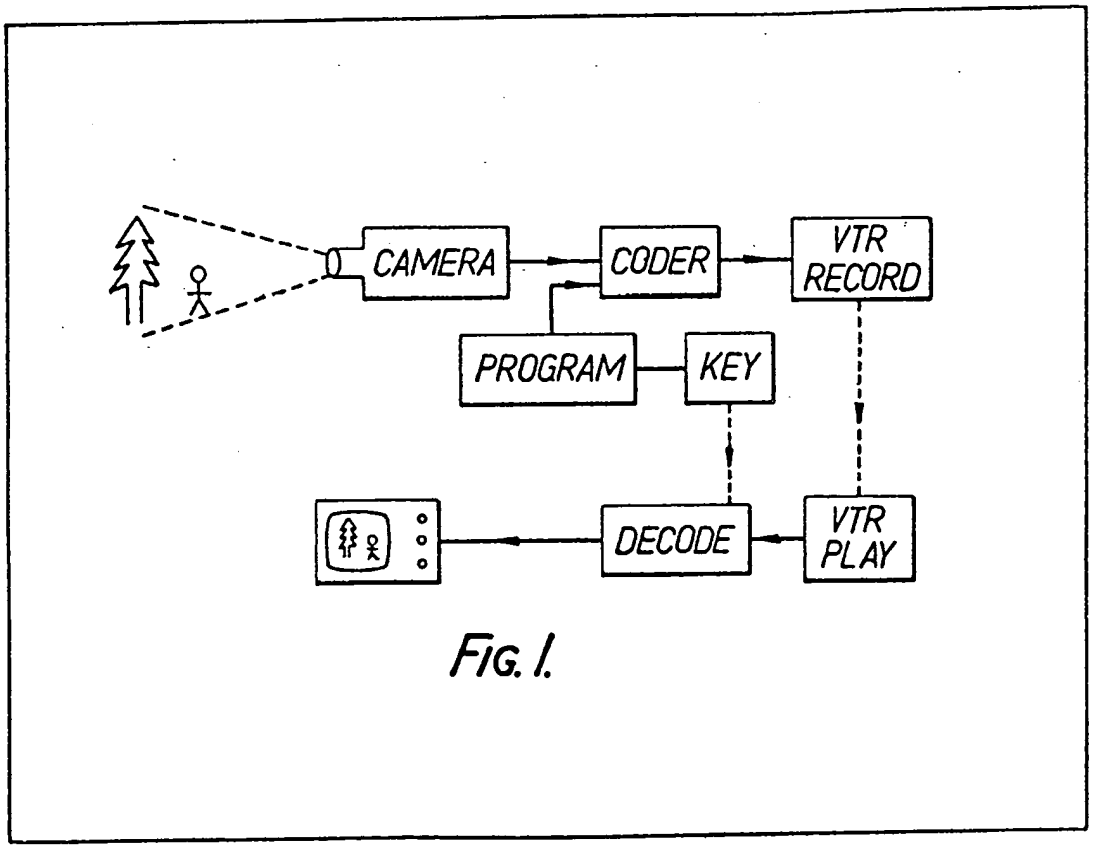

FIG. 1.

GB 2 067 871 A

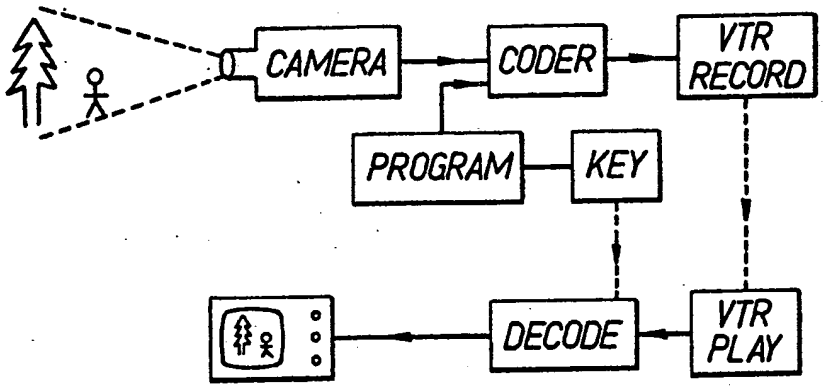

FIG. 1.

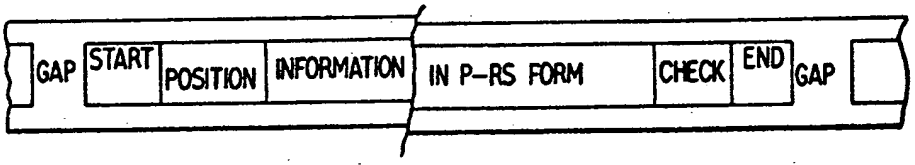

FIG. 2.

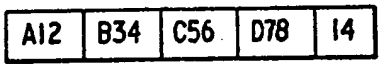

FIG. 3.

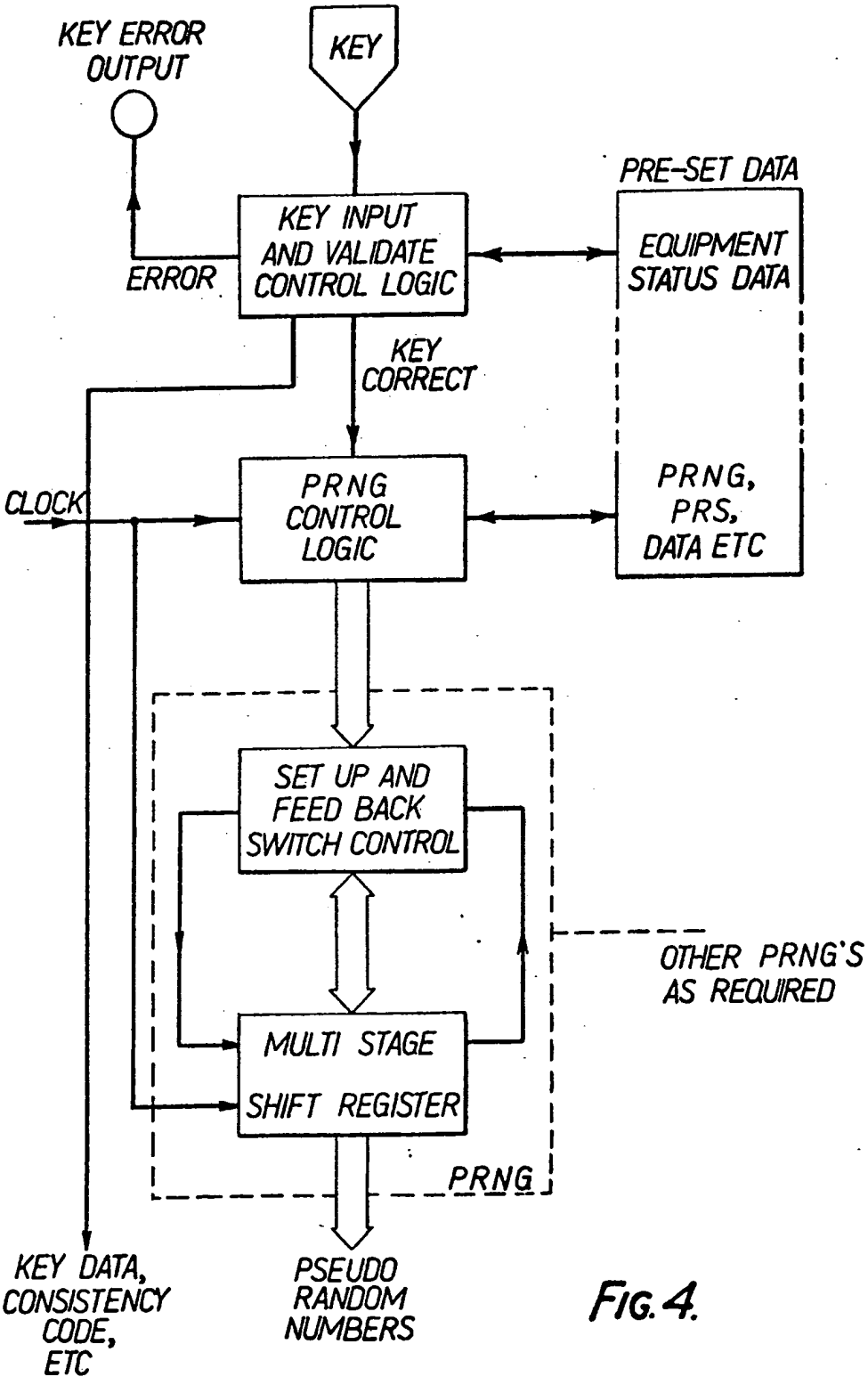
KEY ERROR OUTPUT
KEY
PRE-SET DATA
KEY INPUT AND VALIDATE CONTROL LOGIC
EQUIPMENT STATUS DATA
ERROR
KEY CORRECT
CLOCK
PRNG CONTROL LOGIC
PRNG, PRS, DATA ETC
SET UP AND FEED BACK SWITCH CONTROL
OTHER PRNG'S AS REQUIRED
MULTI STAGE SHIFT REGISTER
PRNG
KEY DATA, CONSISTENCY CODE, ETC
PSEUDO RANDOM NUMBERS

FIG. 4.

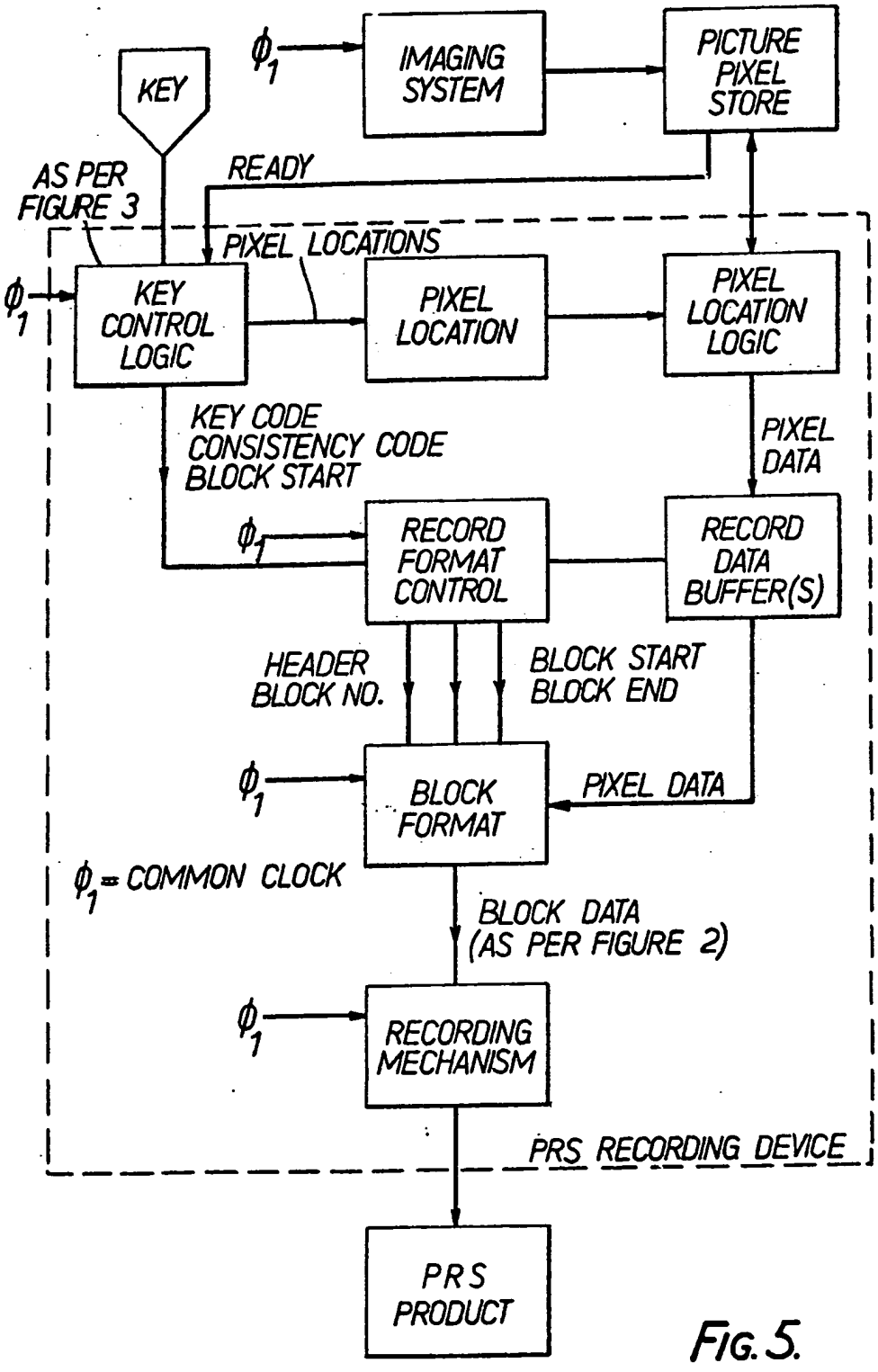
KEY
ϕ_1
IMAGING SYSTEM
PICTURE PIXEL STORE
AS PER FIGURE 3
READY
PIXEL LOCATIONS
KEY CONTROL LOGIC
PIXEL LOCATION
PIXEL LOCATION LOGIC
KEY CODE
CONSISTENCY CODE
BLOCK START
PIXEL DATA
RECORD FORMAT CONTROL
RECORD DATA BUFFER(S)
HEADER BLOCK NO.
BLOCK START
BLOCK END
BLOCK FORMAT
PIXEL DATA
ϕ_1 = COMMON CLOCK
BLOCK DATA
(AS PER FIGURE 2)
RECORDING MECHANISM
PRS RECORDING DEVICE
PRS PRODUCT

FIG. 5.

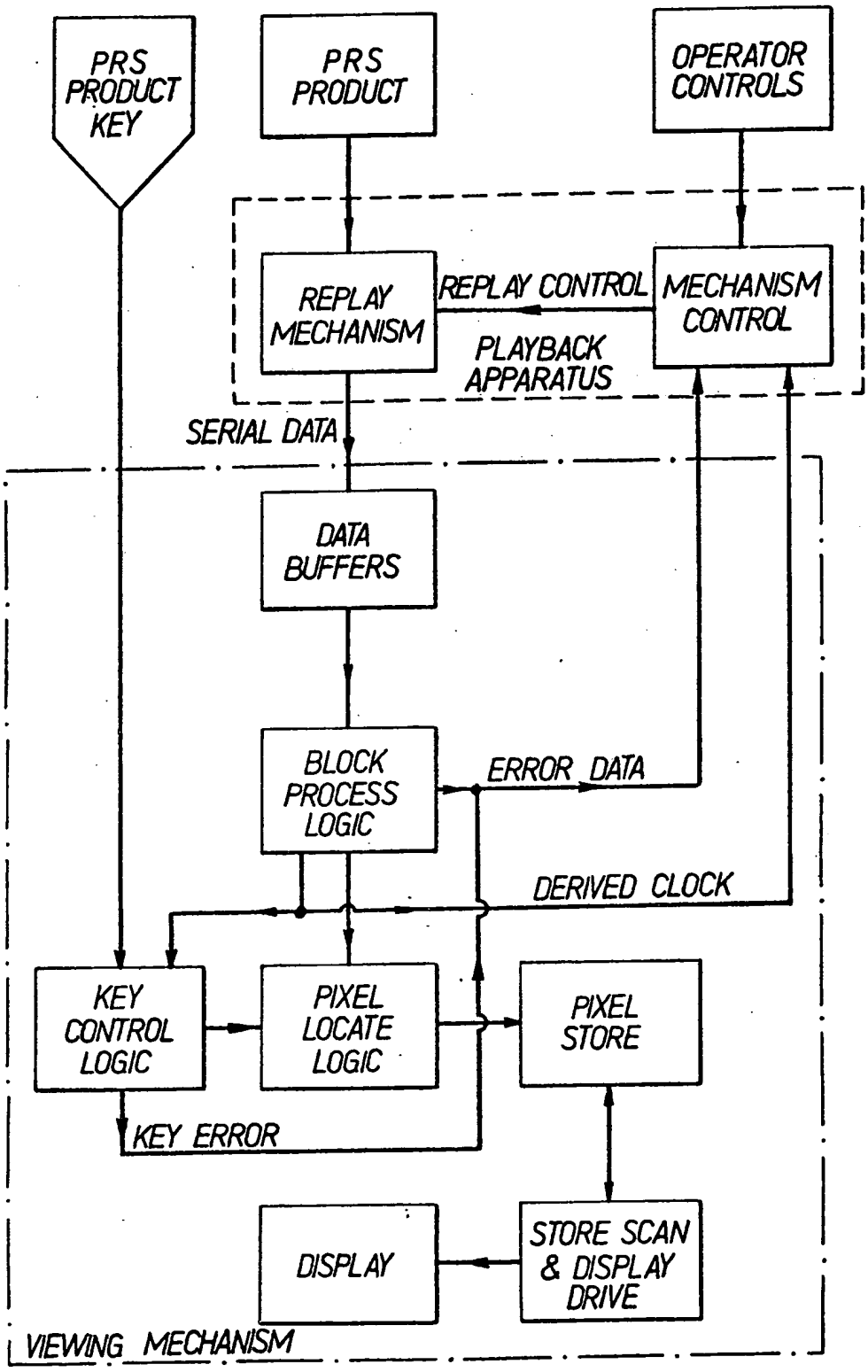
PRS PRODUCT KEY
PRS PRODUCT
OPERATOR CONTROLS
REPLAY MECHANISM
REPLAY CONTROL
MECHANISM CONTROL
PLAYBACK APPARATUS
SERIAL DATA
DATA BUFFERS
BLOCK PROCESS LOGIC
ERROR DATA
DERIVED CLOCK
KEY CONTROL LOGIC
PIXEL LOCATE LOGIC
PIXEL STORE
KEY ERROR
DISPLAY
STORE SCAN & DISPLAY DRIVE
VIEWING MECHANISM

FIG. 6.

SPECIFICATION

Information Encoding Systems

This invention relates to information encoding systems, and concerns in particular methods for the encoding and decoding of information organised in block form.

Information encoding systems—that is, systems for converting information (data) from one form into another—are well-known in a variety of fields. At one level the expression "code" conjures up a picture of espionage, and the sending of secret messages in a coded form intelligible only—it is hoped—to the addresses, while at another level it brings to mind electronics, and the routine conversion of information into a signal (or a series of signals) which itself identifies but does not resemble the original data (such as is very commonly used when information in analogue form is converted into information in digital form). The first of these is all about security, and the encoding serves no other purpose than to disguise the information itself, while the second of these basically concerns the handling of the data, and the information's actual nature is irrelevant.

There are, however, a number of occasions where it is desirable for information encoded in the latter sense also to be coded in the former sense—thus, say, for data which has been put into the form of electronic, magnetic, optical or mechanical pulses to be unintelligible to anyone but the intended recipient of that data. A typical example of such a case is that of videotape recordings and the prevention of their illegal, copyright-infringing, reproduction. It is, unfortunately, common practice for videotape recordings to be "pirated"—that is, for many illegal copies to be made from one legally-acquired copy, and to be sold cheaply, with the result that the copyright owner is deprived of his just reward gainable by selling authorised copies—and it would be useful to have an information encoding system applicable to such an example so as to prevent any videotape being played back to give an intelligible result without first knowing how the recorded signal is to be decoded. The invention seeks to provide such a system based upon a technique known as pseudo-random scanning.

Though first proposed in the 1930's, pseudo-random scanning (p-rs) is in practice a relatively new information-handling technique currently used (or suggested for use) mainly in certain types of television system. It may briefly by explained as follows.

Whereas in a conventional television system the picture (to be taken by the camera, transmitted by the broadcasting equipment, and received and reconstituted by the television set receiver) is scanned in an ordered series of closely-spaced parallel lines called a raster, in a p-rs system the picture is in effect scanned in a sequence of points dotted about apparently at random ("apparently" because, though the sequence may appear to be random, it is not so, and in fact is controlled according to some predetermined programme so as eventually to cover the whole picture).

P-rs systems have a number of significant advantages over comparable conventional raster systems. Specifically, they employ a much lower data rate (as little as one sixth as much) and so require very much less bandwidth, and in addition they are less troubled by noise problems. For both these reasons they find use in satellite and spaceship communication systems.

In a practical p-rs system the picture is first notionally divided into a large number of small picture elements (pixels) arranged in an ordered grid-like matrix, and then these are looked at in a predetermined pseudo-random sequence which (usually, though not always) is constructed so that all of the pixels are examined once and once only in each sequence. The output for each pixel may be in analogue form—the specific value of some variable, such as an electrical voltage, representing (for example) the colour or the brightness of that pixel—but it is in most applications more convenient to have the output encoded into digital (usually binary) form, so that it is obtained as a number indicating the magnitude of the variable(s) concerned. The pseudo-random sequence may be obtained in any one of a number of different ways commonly used to generate random numbers; thus it may be generated using software or hardware, though the latter—especially in the form of the comparatively simple multi-stage feedback shift register circuit—is particularly convenient.

In conventional p-rs systems the actual p-rs sequence is predetermined and constant—indeed, it will probably have been specifically chosen with the particular utilisation in mind—so that the receiving equipment (the television set) can be designed in advance to perform the same p-rs sequence so as correctly to reconstitute the picture in image form.

The present invention seeks to provide a system, using basic p-rs techniques, for the handling of information (especially in picture form) as a series of different prs sequences in such a way as to be unintelligible to anyone without the key defining the different p-rs sequences being employed.

In one aspect, therefore, this invention provides a system for the provision and distribution of information in coded form, in which:

successive blocks of the information are pseudo-randomly scanned, the actual pseudo-random scanning sequence being changed from block to block according to a predetermined but "secret" key, the output from the scanning process constituting the information in coded form; and

the thus-coded information is then distributed in a form which does not include any details which fully define the key, the required key-defining details being themselves distributed separately and independently.

Though naturally this system may be used with any sort of information which is either in, or can be put into, block form (by "in block form" is meant simply in the form of a largish number of basic data elements, like a line or page of print or typing, or a picture) it is particularly applicable to information which takes the form of a sequence of pictures as, for example, produced by a cinematograph film or a conventional television system.

The particular technique used to effect the p-rs can be any such available technique. Depending upon the exact form of the data, however, preferred p-rs techniques involve the use of a hardware approach employing conventional multi-stage feedback shift registers to construct an apparently random sequence of all the numbers between given minimum and maximum numbers; this sequence can be employed to direct the selection of which data element—for example, pixels—to read/write at any given time. The number of each of these numbers should be at least equal to a large proportion—say, a quarter—of the number of data elements in each information block, and is preferably equal to or larger than the number of data elements. Naturally, the number of possible basic sequences is enormous, being limited only by the number of ways of interconnecting the various active elements in the shift register, while in addition every sequence can be initiated at any chosen point in that sequence, so forming a "sub" sequence at first sight quite different to the basic sequence. The generation of pseudo-random number sequences is fully described in Rabiner and Gold, Theory and Application of Digital Signal Processing (Prentice Hall).

Similarly, any of the enormous number of possible p-rs sequences can be used, though again a preference for certain types may exist depending upon the form of the data (for example, to avoid "flicker" problems with pictures it is desirable that the p-rs sequence be "uniform" at least over the centre of the field of the scan, and therefore it may be preferred in such cases to use a p-rs sequence which is constrained to repeat a portion of the sequence covering the centre field).

In the system of the invention the p-rs sequence used is changed "from block to block". It should here be pointed out that a block does not necessarily have to correspond to any single naturally-occurring piece of information (as a single picture) but may instead correspond to groups of such items (as several pictures) or even parts or fractions thereof (as half a picture, or a picture-and-ahalf). Moreover, no one block need be the same "size" as any other block (specifically, as its two neighbouring blocks). Thus, for instance, a first block might constitute a single picture, whilst the second and third blocks constitute four and two pictures respectively. Accordingly, it will be understood that the expression "block" is arbitrary as regards its relation to the information it contains; the method of the invention merely requires that the p-rs sequence used change—and change reasonably often—as the coding process progresses. In fact, of course, for most purposes the blocks will correspond to natural information items (single pictures, say), though in a practical situation it can be arranged that the actual changeover from one p-rs sequence to another is purely time-dependant (so that the block size may become quite arbitrary).

The frequency with which the p-rs sequence changes is conveniently such that each block is a very small proportion—a thousandth, or a millionth—of the whole. This clearly renders the encoded information much more difficult to decode without the key. However, this does not necessitate the use of a comparable number (a thousand, or a million) p-rs sequences; indeed, such complexity might make the coding key impossibly long. Instead, it is envisaged that the number of p-rs sequences used in any one coding operation would be low (a hundred, say), but that they would be repeated—possibly in a second pseudo-random sequence—and that the key would identify not only which p-rs sequences were to be used but also in what order and re-order they were to be used.

Prior to distribution of the information within each block coded in accordance with the system of the invention there is most conveniently impressed upon that information additional, control, data identifying various features thereof. Specifically, for example, each block is preceded by data indicating a) the start of the block (mainly for synchronisation purposes), and b) the position of that block in the current sequence of blocks (for the purpose of selecting the correct p-rs decoding sequence for that block). Similarly, each block is terminated by an end-of-block signal (again, mainly for synchronisation purposes, though it could also include a check portion relating to the detection and correction of errors in the data in the block). Between blocks there can either be an actual gap—an absence of any data transmission—or a "null code" indicating that there is a gap in the information.

The key required for the system of the invention primarily identifies the p-rs sequences used for the actual coding stage, and so to be used for the decoding, and in a preferred method (in which the actual p-rs sequences repeat themselves) it also identifies the series of p-rs sequences presently in use. It should perhaps here be emphasised that the key is distributed separately and independently of the encoded information (and any control data impressed thereon).

As will be appreciated, the format of the key may be of any suitable type, but preferably the key will itself consist of a series of data elements divided up into segments ("fields") each of which identifies a particular feature enabling the correct p-rs sequence to be employed. For example, one field could identify the equipment for which the key is effective (with specific reference to the available p-rs sequences), another field could

identify the particular entry in a table defining a particular set of particular p-rs sequences among the available sets of sequences, while yet another field could identify the starting point to be used with the chosen p-rs sequences. A further field could be used as a check on consistency (as between the key, the control logic equipment, and the information product), while another field could be a validation check on the value of the key itself.

Naturally, the actual nature of the key—for example, whether it is wholely numerical or perhaps alphanumerical, the number of fields it contains, and the order and size of those fields—may be any that is appropriate.

It will be seen that one aspect of the invention is an information coding, distribution and decoding system wherein:

For Coding and Distribution

a) the information is divided into a series of blocks, and the information in each block is coded using pseudo-random scanning techniques, the actual pseudo-random scan sequence being predetermined, and being changed from block to block in a predetermined (possibly pseudo-random) manner,

b) the information in each coded block is preceded and followed by extra data portions identifying the start and end of that block, and the position of the block within the series of blocks,

c) the actual pseudo-random scan sequence for each block, and the series of such sequences, is each identified by a segment of an encoding key, which key is separate from the encoded information and its associated extra data portions, and

d) the encoded information, together with the extra data portions, is distributed separately and independently of the related key; and

For Decoding

e) from each extra data portion there is obtained the start time for the block, coupled with a positional factor relevant to that block,

f) using that factor there are selected from the pseudo-random scan sequences located by the key the particular pseudo-random scan sequence(s) relevant to that block, and

g) using the appropriate pseudo-random scan sequences each coded information block is then decoded using pseudo-random scanning techniques, and presented in succession to give the desired information in plain form.

The system of the invention is applicable to information recorded in anyway whatsoever—for example, as electronic pulses in a microprocessor read-only-memory (ROM), as magnetic pulses on a magnetic tape, as optical pulses on a film strip, or as mechanical pulses on a gramaphone record. However, it is seen as being of particular value in connection with the prevention of the unauthorised reproduction of copyright material in that form of magnetic pulses on a magnetic tape known as a videotape recording. Thus, in a more limited aspect the invention provides a system enabling the recordal and playback of information so as to prevent or hinder the unauthorised reproduction of that information by playing back the formed record, in which system:

a) the information is arbitrarily divided into a series of blocks each of which contains a portion of the information as an ordered sequence of information elements;

b) the sequence of each block is then sampled, using pseudo-random scanning techniques, to produce a second sequence in which the information elements are now in an apparently random but nevertheless predetermined, known order;

c) the second, random sequence is then recorded, a note being made of the actual random sequence so that the playback apparatus may be suitably programmed to reproduce that random sequence when playing back that block, this recordal stage being effected for each block random sequence in turn so as to provide a recording of the entire series of blocks, the series of such notes for the series of random sequences (no two successive blocks of which are random in the same identical way) for the series of blocks constituting a quite separate "key" (or part of a key) whereby the playback apparatus may be programmed for the entire series of blocks; and

d) upon playback of the formed record using the appropriate apparatus the information in its original ordered sequence can only be obtained by first using the separate key to programme the apparatus to read the recorded information elements for each information block in the correct random sequence for that block.

Such a system might be of value in the following scheme for the sale/rent of videotape recordings.

Firstly, the potential law-abiding customer acquires a television set and video tape playback apparatus capable of using p-rs techniques. Secondly, the customer buys (or rents) the required videotape (which has been recorded in accordance with the inventive system), together with an appropriate "ticket" enabling him to obtain the coding key for that particular videotape recording. Thirdly, using his "ticket" as proof of entitlement the customer acquires—from a separate source—the coding key specific to his videotape recording. Fourthly, the customer uses the coding key to adjust his equipment to scan in the p-rs sequences specific to his particular videotape recording.

Certain embodiments of the invention will now be described, though only by way of illustration, with reference to the accompanying drawings in which:

Figure 1 shows in schematic form an overall representation of a simplified coding/decoding system of the invention as applied to videotape recordings;

Figure 2 shows diagrammatically a length of videotape, visuallizing the data carried thereby, for use in the system of Figure 1;

Figure 3 is a pictorial representation of an

encoding/decoding key for use in the system of Figure 1;

Figure 4 is a schematic block diagram of a key control logic arrangement for use in the system of Figure 1;

Figure 5 is a schematic block diagram of a tape recording stage for use in the system of Figure 1; and

Figure 6 is a schematic block diagram of a tape playback stage for use in the system of Figure 1.

The system of the invention when used in connection with videotape recording operates overall in the manner shown (in simplified form) in Figure 1. A TV camera views the chosen scene and provides a conventional raster output. This output is fed to an encoder which uses p-rs techniques to convert its original raster input to a "random" output according to its programmed instructions. The output is recorded, and the programme of coding instructions is separately available in the form of a key which can subsequently be used for decoding the "Random" Output.

The tape record of the "randomised" picture is sold to the customer, who separately obtains the key (which very possibly is unique to that actual tape), and plays the tape back through his decoder after programming it with the key.

The playback apparatus provides a "random" output which is fed to the decoder. The decoder (here shown as a separate item, though it may be preferable to build it into—and as an integral part of—the television set), which is loaded with various p-rs sequence sets amongst which is the relevant one, uses the key to select the correct p-rs sequence for each information block, and provides as its output a decoded, raster-type signal which can be fed directly into a conventional TV receiver to produce an image of the original chosen scene.

The length of videotape shown in Figure 2 bears information which can be visuallized in the manner pictured. The tape travels from right to left, and so is read from left to right. After the left-hand information block there is a gap—a length of tape bearing no signal whatsoever—followed by the next block. This block (and all of the blocks) comprises five distinct groups of data. First, there is a "start of block" data element, this ensures that the decoder is set up to use a whole new p-rs sequence. Second, there is a "block position identifier" data element; this gives the position of the block in the series of blocks, and is used by the decoder, in conjunction with the key, to select the correct decoding p-rs sequence(s) for that particular block. Third, there is the information being replayed—in this case data concerning the pixels into which the original raster image was divided—in a pseudo-random order. Fourth, there is a "check" element; this is used to detect and correct errors in the block. Last, there is the "end of block" element; this signals the end of that part of the playback operation, and readies the equipment for a new block. This "end of block" element is followed by a gap, and then by the next block.

In Figure 3 there is shown a pictorial representation of an alphanumeric coding/decoding key. The key is shown divided into five fields; these determine, respectively, the set of p-rs sequences used (A12), the start point taken for each p-rs sequence (B34), the equipment status on which this key is effective (C56), the consistency between key, control logic and information product (D78), and a pair of check digits for validation of those in the previous fields.

Figure 4 shows in schematic block diagram form a key control logic layout for pseudo-random number generation.

The key is input, and the key data is checked for validity; if correct, this key data is used in the pseudo-random number generator (PRNG) control logic to access preset data which defines the ordering of the or each pseudo-random number sequence, the sequence and the starting point for potential keys. For each pseudo-random number sequence the PRNG control logic configures the multi-stage shift register to generate the correct sequence by switching the feedback paths between the shift register stages. The PRNG control logic loads the multi-stage shift register to the desired starting value in the pseudo-random number sequence as defined by the starting point data by setting appropriate bits in each stage of the shift register. The multi-stage shift register is now ready to generate a pseudo-random number sequence, and a new pseudo-random number is generated with each clock signal.

The data defining the ordering of the pseudo-random number sequences is used in the PRNG control logic to reconfigure the multi-stage shift register when the limit to the current sequence is reached. For convenience, more than one reconfigurable multi-stage shift register may be used, so that the PRNG control logic could set up the subsequent PRNG(s) whilst using the current PRNG for the generation of a sequence of pseudo-random numbers which define the location of the pixel to be used.

The block diagram of Figure 5 represents a tape recording stage in the inventive system.

The key is decided in advance, and input to the recording control logic. The total control logic at this stage is more complex than that described for generating pseudo-random sequences from the key in the key control logic and is an integral part of the recording mechanism. A common—master—clock is used to derive the necessary clock signals for the imaging system, the control logic and the recording mechanism (if separate).

The imaging system produces a picture image which is stored in pixel cellular structure in the picture store using established picture scan, sampling and storage techniques. Once the picture store is initially filled a start signal is returned to the control logic, which generates a number of signals—viz, a consistency check derived from the key, the location of the pixel to

be accessed, and a block start code to the recording device. The recording device incorporates a data buffer (or buffers) to assist in the appropriate formatting of pixel data into blocks. Thereafter each clock signal causes the p-rs pixel location to be generated, the contents of that location being transferred to the recording device. As each block of data is completed it is recorded in a format similar to that in Figure 2. There will be a maximum length to a block, and the check digits are automatically added to incorporate some degree of error recovery. A new block will always be started every time the p-rs in use is changed even if the maximum length has not been reached, and each block carries its own identifier or block number. This identifier is automatically generated by the control logic within the recording device or the key control logic.

The recording device produces the equivalent of the videotape recording, and this product now has to be reconstructed to be viewed. This is effected using a replay and view stage as shown in Figure 6.

The playback apparatus *per se* is a comparatively simple mechanism capable of reading the videotape recording and transferring the read serial data to the viewing apparatus at a rate consistent with the latter's ability to present it.

Prior to replaying a tape, the key is input to the viewing apparatus where the latter's key control logic checks the key for consistency, then, when the product is being replayed, also checks the serial data for consistency—so there is a series of cross checks throughout. The viewing apparatus has very complex logic in addition to the key control logic. Probably the most significant feature is the clock. This operates at a nominal frequency, but is synchronised to the replay data rate. As the data is being received from the playback apparatus the control logic uses the block number to compare that the correct p-rs setting is in use, and with subsequent pixel data locates each data item, at the location derived by the key control logic, in the picture store. This store is then raster-scanned in the conventional manner to produce the viewable image.

The viewing apparatus itself processes the serial data stream from the playback apparatus, removing the "start of block" and "block terminator" features, etc., and checking the block data against the check digits. Simple errors are recoverable by use of a data buffer and error correction codes. Complex errors are less likely, and will normally be ignored on a single block basis: continuing errors are obviously a sign of some fault in the equipment. So that complex errors can be tolerated the block sequence identifier is necessary. This enables the key control logic directly to relate to the p-rs sequence in use for each block by computation from the key (the 'synchronisation' referred to earlier). Starting and stopping in replay is achievable, as is running at a slower speed, which slows the clock; for each element of pixel data in each block the key control logic can compute the correct location for it to be stored in the picture store. "Freeze Frame" is simply no update to the picture store, so a constant viewable image can be maintained.

In a cable television type of application the block sequence identifier enables the receiver to join the system at any time. In this case there would be no key/product consistency check unless each block included an identifier for checking. In a practical system there might have to be a minor delay until a new p-rs sequence came into use, and thus the viewer might miss a few moments of viewable data. Again, the block identifier could include a feature to indicate that for this block a new p-rs sequence is to be used, rather than a continuation of a previous one where it might not be possible to determine how many stages it should have clocked through and thus where in the p-rs sequence the locations are.

Claims

1. A system for the provision and distribution of information in coded form, in which:

successive blocks of the information are pseudo-randomly scanned, the actual pseudo-random scanning sequence being changed from block to block according to a predetermined but "secret" key, the output from the scanning process constituting the information in coded form; and

the thus-coded information is then distributed in a form which does not include any details which fully define the key, the required key-defining details being themselves distributed separately and independently.

2. A system as claimed in claim 1, applied to information which takes the form of a sequence of pictures.

3. A system as claimed in either of the preceding claims, in which the technique used to effect the p-rs involves the use of a hardware approach employing conventional multi-stage feedback shift registers to construct an apparently random sequence of all the numbers between given minimum and maximum numbers.

4. A system as claimed in any of the preceding claims, in which the number of each of the random numbers in any one sequence of random numbers is equal to or larger than the number of data elements in the block to which that sequence is applied.

5. A system as claimed in any of the preceding claims, in which the p-rs sequences used with picture data are "uniform" at least over the centre of the field of the scan.

6. A system as claimed in any of the preceding claims, in which the number of p-rs sequences used in any one coding operation is low, but they are repeated, the key also identifying in what order the re-order the sequences are to be used.

7. A system as claimed in any of the preceding claims, in which, prior to distribution of the information within each block coded in

accordance with the method, there is impressed upon that information additional, control, data indicating a) the start of the block, b) the position of that block in the current sequence of blocks, and c) and end-of-block signal.

8. A system as claimed in any of the preceding claims, in which the key itself consists of a series of data elements divided up into segments each of which identifies a particular feature enabling the correct p-rs equence to be employed.

9. A system of coding information as claimed in any of the preceding claims and substantially as described hereinbefore.

10. An information coding, distribution and decoding system wherein:

For Coding and Distribution

a) the information is divided into a series of blocks, and the information in each block is coded using pseudo-random scanning techniques, the actual pseudo-random scan sequence being predetermined, and being changed from block to block in a predetermined (possibly pseudo-random) manner,

b) the information in each coded block is preceded and followed by extra data portions identifying the start and end of that block, and the position of the block within the series of blocks,

c) the actual pseudo-random scan sequence for each block, and the series of such sequences, is each identified by a segment of an encoding key, which key is separate from the encoded information and its associated extra data portions, and

d) the encoded information, together with the extra data portions, is distributed separately and independently of the related key; and

For Decoding

e) from each extra data portion there is obtained the start time for the block, coupled with a positional factor relevant to that block,

f) using that factor there are selected from the pseudo-random scan sequences located by the key the particular pseudo-random scan sequence(s) relevant to that block, and

g) using the appropriate pseudo-random scan sequences each coded inforation block is then decoded using pseudo-random scanning techniques, and presented in succession to give the desired information in plain form.

11. A system as claimed in claim 10 which is for the recordal and playback of information so as to prevent or hinder the unauthorised reproduction of that information by playing back the formed record, in which system:

a) the information is arbitrarily divided into a series of blocks each of which contains a portion of the information as an ordered sequence of information elements;

b) the sequence of each block is then sampled, using pseudo-random scanning techniques, to produce a second sequence in which the information elements are now in an apparently random but nevertheless predetermined, known order;

c) the second, random, sequence is then recorded, a note being made of the actual random sequence so that the playback apparatus may be suitably programmed to reproduce that random sequence when playing back that block, this recordal stage being effected for each block random sequence in turn so as to provide a recording of the entire series of blocks, the series of such notes for the series of random sequences (no two successive blocks of which are random in the same identical way) for the series of blocks constituting a quite separate "key" (or part of a key) whereby the playback apparatus may be programmed for the entire series of blocks; and

d) upon playback of the formed record using the appropriate apparatus the information in its original ordered sequence can only be obtained by first using the separate key to programme the apparatus to read the recorded information elements of each information block in the correct random sequence for that block.

12. An information coding distribution and decoding system as claimed in either of claims 10 and 11 and substantially as described hereinbefore.

Printed for Her Majesty's Stationery Office by the Courier Press, Leamington Spa, 1981. Published by the Patent Office, 25 Southampton Buildings, London, WC2A 1AY, from which copies may be obtained.